Section:	06	Title:	Information Security
Sub Section:	03	Title:	Information Security
Document:	08	Title:	Cryptography, Electronic Signature

1. STANDARD

ISD will implement authentication functions that are consistent with the level of confidentiality or sensitivity of the information they contain or process.

1.1. Summary of Standard Changes

1.2. Purpose

To insure the authentication and confidentiality of information.

1.3. Scope

Applies to all information or processes deemed sensitive.

1.4. Responsibilities

1.5. Definitions and Abbreviations

1.6. Description of Standard

Risk analyses on information and processes will determine which elements should be encrypted or posses digital signatures in order to provide authentication confidentiality whether being transmitted, stored, or transacted upon.

1.7. Implications

Sensitive information will be guaranteed that it originated with a specific sender, has not been changed, is received in the same sequence as transmitted, and is delivered only to the intended receiver.

1.8. References

1.9. Attachments

2. RISK ANALYSIS PROCEDURES

2.1. Summary of Procedure Changes

2.2. Procedure Details

2.2.1. All ISD information resources and process will have risk assessment to determine their level of sensitivity and authentication devices need. Any necessary devices will be procured.

2.2.2. Results of the analyses with authentication requirements are communicated to personnel along with necessary training on any device or process.

2.2.3. Necessary monitoring of information and processes by ISD Security will be performed to insure compliance with directives.

2.3. References

2.4. Attachments

3. ENCRYPTION PROCEDURES

3.1. Summary of Procedure Changes

3.2. Procedure Details

3.2.1. Cost benefit analyses of risk assessments on ISD resources and process is used to define the encryption device to be used.

3.2.2. All information storage media (such as hard disk drives, floppy disks, magnetic tapes, and CD-ROM’s) containing sensitive information will be physically secured when not in use. An exception will be made if this information is protected via an encryption system approved by ISD security.

3.2.3. No sensitive information will be transmitted over any communication network except in encrypted form.

3.2.4. ISD will use a public key encryption system.

3.3. References

3.4. Attachments